J. Appl. Environ. Biol. Sci., 4(7S)342-349, 2014

© 2014, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

An Efficient and Secure Cluster-Based Architecture for AMI Communication in Smart Grid

Asfandyar Khan, Nizamuddin, Jawaid Iqbal, Noor Ul Amin

Department of Information Technology, Hazara University, Mansehra, Pakistan

Received: September 1, 2014
Accepted: November 13, 2014

ABSTRACT

Smart Grid has revolutionized Traditional Grid System by merging bi-directional communication network and information technology. Advanced Metering Infrastructure (AMI) is an integral part of Smart Grid used to measure power consumed and demands at consumer-end. In this article, we propose an efficient and secure cluster-based architecture for AMI in Smart Grid, which fulfills the primary security requirements like confidentiality, authentication and integrity. Analysis shows that the proposed secure architecture for AMI in Smart Grid is efficient in terms of resource utilization.

KEYWORDS: Smart Grid, AMI, Smart Meter, Cluster, Elliptic Curve

1 INTRODUCTION

Today’s world is facing enormous problems including energy on top in the list. Energy has become the basic need of human being in every domain of life. The Traditional Power Grid System is responsible to provide such energy at the consumer-side. The current Grid System is older more than 100 years and has limitations making it inefficient and unreliable to cope with faults, failures, outages, power demands and energy storage problems etc. So we need a stronger and smarter electric Grid System that will provide abundant, affordable and clean electricity to consumers efficiently, reliably at anytime, anywhere i.e. a 21st Century Grid System also called Smart Grid [1], [2], [17] depicted in Fig1. Smart meters [3]are used to collect, measure, analyze electricity on regular intervals and also collaborate with each other to exchange real time data through a two-way communication network referred as Advanced Metering Infrastructure (AMI). AMI plays an important role in Smart Grid communication network and has gotten much more attention from both industry and academia in recent years. Since electricity is generated, transmitted and distributed at consumer-side on the real time estimates received from AMI networks in Smart Grid, various security and privacy threats [4], [5] have been launched from inside and outside the network by attackers. Inadequate security measures will allow adversaries or attackers to access consumer power profiles, grid power schedules and load management. Further injecting false readings and demands will degrade Grid performance leading to financial loss, causing failures, outages and will create mistrust between consumer and utility company. Secure AMI communication in Smart Grid is a core category for research community. In this paper, we first developed an efficient clustering architecture for AMI communication in Smart Grid, in which cluster formation with cluster-head selection and rotation is performed by centralized clustering algorithms. We use hybrid cryptosystem based on Elliptic curve and Advanced Encryption Standard (AES) for secure and reliable AMI communication in Smart Grid which results in reducing computational as well as communication cost.

The remaining paper is structured as: In Section II we review related work done in past as well as in recent times. In Section III, a brief overview of general Smart Grid architecture is given, in Section IV we propose communication architecture for AMI with security scheme and in Section V; Security Analysis is given and in section VI, we finally draw the conclusion.

2RELATED WORK

In this paper, we have reviewed recent research work to find out which communication architecture fulfilling security requirements for AMI communication in Smart Gridare proposed.

* **Corresponding Author:** Asfandyar Khan, Department of Information Technology, Hazara University, Mansehra, Pakistan.

In [6], a secure and privacy preserving communication scheme is proposed for a wireless mesh network established between smart meters and collector nodes. Devices (smart meters) identities are checked before joining the communication network while Pallier Cryptosystem coupled with digital signature is applied to secure data communication and verify message integrity and authenticity. A secure and reliable scheme is proposed in [7] for a tree-based topology in which data integrity, privacy and confidentiality are achieved through message encryption algorithms and authentication techniques by using mutual authentication. In [8]**,** a light-weight key scheme is proposed for AMI while focusing on HAN (Home Area Network) to design both pair-wise keys and group IDs keys for a large number of entities bearing small overhead. An efficient and privacy preserving scheme is proposed in [9], in which data is encrypted by Homomorphic Pallier cryptosystem. Data aggregation is performed at Gateway without decryption of cipher texts of smart meters while original message will only be obtained in OA (operation center). This scheme achieves user's privacy and resists against security threats with low computation and communication overhead. In [10], has proposed an efficient and key management for Smart Grid communication. In the first step, smart meter of Home Area Network (HAN) and Authentication Server (SAS) of smart Grid mutually authenticate each other by using a Secure Remote Password (SRP) which initialize a password reducing the steps from five to four and packets exchange will decrease from four to three. For secure communication in Smart Grid, a secure key management protocol was proposed i.e. Enhanced Identity Based Cryptography using Public Key infrastructure which will result in preventing various attacks and will reduce management overhead i.e. substantially reduces the overhead of key renewals also. The proposed secure protocol works on a multigate mesh network architecture. In [11], has proposed a lightweight authentication scheme using Diffie-Helman Key establishment and hash-based authentication code for a secure and reliable communication of Smart Grid. The communication network consists of HAN (home area network) at the consumer-end, where smart home appliances sends their data to smart meter, while a BAN GW (Gateway) receives readings from smart meters of HANs, NAN i.e. Neighborhood Area Network at the control center (upper end of Smart Grid) identify a particular region or locality. The proposed protocol provides better security with low latency while few message exchanges occurs in communication process. A security protocol IAC (Integrated, Authentication and Confidentiality) for AMI is proposed in [12], which works on the topology that consist several trees each rooted at feeder. In this scheme, first mutual authentication between smart meters and authentication server is established and then a collaborative data aggregation and forwarding scheme is introduced. A BNS (backbone node selection) algorithm is used for the selection of backbone node in the tree topology and will be reconstructed incase of failure. Data integrity and authentication is achieved through message encryption and authentication techniques during the mutual authentication key establishment.

3 Smart Grid Architecture

General communication architecture of Smart Grid is shown in Fig.1.

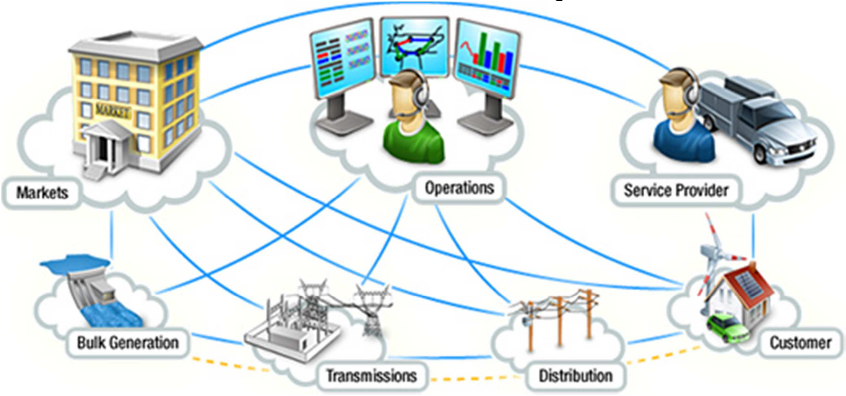

Figure. 1 Smart Grid Communication Architecture

3.1 Smart Home

Electricity is generated, transmitted, distributed and finally provided at smart home (consumer-side) where smart appliances like refrigerator, washing machine, microwave oven, electric fans, light bulbs etc send their power consumptions, future power demands and other status reports to a smart meter over a wireless communication channel like Zigbee[13] or power career line (PLC)[13].

3.2 Smart Meter

At smart home (consumer-side) an advanced metering device is installed by the service provider responsible to send information received from smart appliances to a Gateway through a two-way communication network using communication technologies in [13].

3.3 Gateway

Gateways are installed in each Residential Area (RA) by the service provider which receives information from smart meters, combine and send forward to a local management office (feeder) of the utility company and vice versa.

3.4 Internet Service Provider

Internet Service Providers (ISP) allocates bandwidth to these Gateways over a fast speed dedicated lines like DSL or Fiber Optic technology.

3.5 Operation Center

Information received at local management office by computer system are aggregated and further send to central SCADA(Supervisory Control And Data Acquisition) at Operation Center which provides monitoring, reporting, billing, supervision and generation of power on estimated demands received from consumer-side.

4 Proposed Cluster-Based Architecture for AMI

We proposed a dynamic cluster-based architecture for AMI communication in Smart Grid as shown in Fig.2, and consist of the following setup phases.

- Advertisement Phase
- Joining\Registration Phase
- Smart Meters Verification Phase
- Cluster Formation with Cluster-Head Selection Phase
- Clusters Completion Phase
- Secure Data Communication Phase
- Cluster-Head Rotation Phase

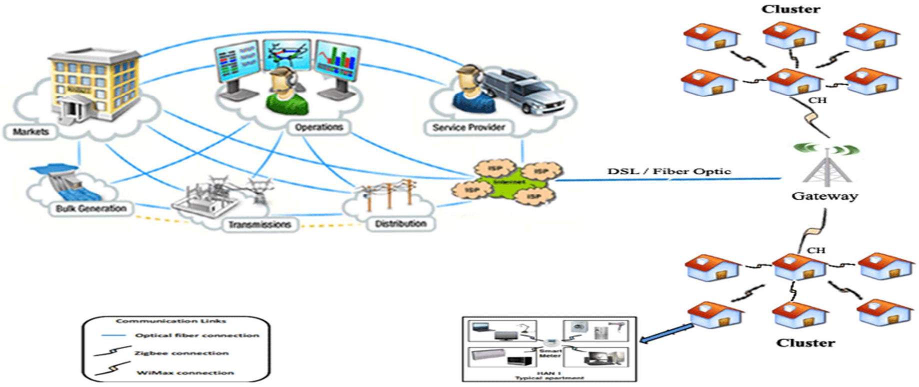

Figure. 2. Communication Architecture for AMI

Table 1: Consists of notations used in this paper.

Table1. Notations Guide

Notation	Explane
N	Total smart meters in RA
S	Verified List of smart meters
RA	Residential Area
SM	Smart Meter
RF	Radio Frequency
Pu	Public Key
Pr	Private Key
Rn	Random Number
H	Hash Function (SHA 128)
C	Cipher Text
E	Encryption
D	Decryption
CH	Cluster-Head
$\mathbf{K_{ses}}$	Session Key

4.1 Assumption

Let that there are "N" homogeneous smart meters (SM_1 …SM_N) in a $M \times M$ residential area equipped with an RF communication transceiver and in good communication range of Gateway. All these smart meters are fixed i.e. non-movable and receive continuous power.

4.2 Advertisement Phase

Gateway sends out an Advertisement (Discovery) message to all SMs in the Residential Area containing (Gateway ID, Public Key $_{\text{Gateway}}$) depicted in Fig.3.

4.3 Registration Phase

Upon receiving Advertisement message, each SM_i sends back a Join Message containing ($MeterID_i, (X_i, Y_i) andRandomNumber$) to Gateway in a secure mode. We assumed that all these SM_i and Gateways are preloaded with public and private keys whereas their public keys are also stored on Authentication Servers at local management office as well as computer servers at Operation Center depicted in Fig.3.

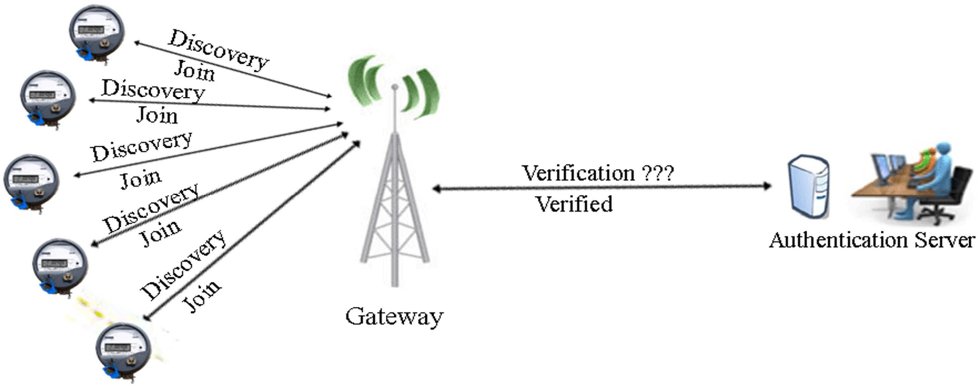

Figure. 3. Smart Meters Advertisement & Registration Phase

Step 1Smart Meter Encryption

$$\text{Input} = (\text{Rn} \,||\text{Location} \,||\text{Meter ID}) \qquad (1)$$

$$\text{hi} = \text{H}(\text{Input}) \qquad (2)$$

$$\text{C}_\text{i} = \text{E}_{\text{PuGateway}}\ (\text{Input} \,||\text{hi}) \qquad (3)$$

EachSM$_\text{i}$calculateC$_\text{i}$ and send to the Gateway in Join Message.

4.4 Smart Meters Verification Phase

We assumed that these Gateways are honest and secure from attackers. The C_i received by Gateway from SM_iwill be decrypted as:

Gateway Decryption

$$D_{PrGateway}(C_i) \qquad (4)$$

$$\text{Compute } hi' = h(Rn\,||Location\,||Meter\ ID) \qquad (5)$$

If hi'=hi valid otherwise invalid

Step 2 Verification

A list of smart meters (valid) is formed and send forward to authentication computer at local management office to further verify their Meter IDs that is already stored on these computer system of the utility company.

Step 3

The verified list "S" of smart meters is send back to the Gateway by the Authentication Computer.

Step 4 Smart Meters Distance Measurements

Distance will be measured for each SM_iin "S" from their corresponding co-ordinates received in registration phase by Gateway using the following distance formula as:

$$d_{GW,i} = \sum_{i=1}^{S} \sqrt{(X_{GW} - X_{SMi})^2 + (Y_{GW} - Y_{SMi})^2} \qquad (6)$$

4.5 Clusters Formation with Cluster-Head Selection Phase

For optimal clusters formation in "S", let k will be the average number of SM_iin each (S/k) clusters containing one Cluster-Head (CH) and ((**S**/***k***) -1) non-Cluster-Head members. The criterion for the selection of being first CH in a cluster is that a member having minimum distance to Gateway. Following pseudo code in algorithm.1 performs Cluster formation with Cluster-Head selection as:

Following algorithm.2 performs CH rotation as:

Algorithm1. **Clusters Formation with Cluster-Head Selection**

```
Input:  Read S, k
Initialize Clusters =:0
If  (S mod k ==0)  Then
Clusters=: S/k
Else
Clusters=: (S/k) + 1
End if
Initialize j=:1;  ctr =:1
Label:              For  (i=:1 To clusters) do
While (j <= Meter Loc .Upper bound) do
Initialize MNo =:0
MNo =: Meter Loc$_{Meter\ No\ j}$
C$_{i, Meter\ ID\ ctr}$=: MNo
If (Ctr==1) then
CH$_{i, Meter\ ID\ ctr}$=: MNo
Else  If (ctr==k) then
j =: j+1; ctr =:1
Exit While
GoTo Label
ElseIf (ctr<= k&& j== Meter Loc .Ubound) Then
Exit While
GoTo Label
Else
j =: j+1
ctr =: ctr +1
End If ; End If; End If
End While
End For
Return C$_{i, Meter\ ID\ ctr}$ , CH$_{i, Meter\ ID}$
```

4.6 Clusters Completion Phase

Finally, Clusters will be completed in the following steps as:

Step1 Cluster-Head Announcement

Now Gateway will send out Announcement Message to each CH containing CH Meter ID and TDMA schedule.

Step2 Each CH will send back a Join Message to Gateway.

Step3 Each CH will send a Hello Message to its corresponding cluster members containing a TDMA schedule to determine a predefined transmission slot to avoid collisions.

Step4 Synchronization

We assumed that cluster members are synchronized and this will be achieved by Gateway sending synchronization signals to each member at the start of cluster formation phase.

4.7 Secure Data Communication Phase

Secure AMI communication will bring stability to Smart Grid network. In recent years, AMI networks have faced numerous cyber attacks. Different security schemes have been proposed for reliable and secure Smart Grid communication. Our security scheme works as follow:

4.7.1 Session Key Generation by Gateway

For Session Key(K_{ses}) generation, Gateway randomly selects two random numbers from the list $(R_{n1}, R_{n2}, R_{n3} \ldots R_{nn})$takes its XOR and calculates the Session key for a cluster as:

Step1$K_{ses} = (R_{ni}\ \mathrm{XOR}\ R_{ni})$ (7)

Step2 $C_{K_{ses}} = \mathrm{ERni}(K_{ses}||\mathrm{CHMeterID})$ (8)

Step3 Gateway will send encrypted Session key $C_{K_{ses}}$ to each corresponding SM_i

4.7.2 Decryption of $C_{K_{ses}}$by rt Meter(SM_i)

Step1 EachSM_iwill decrypt the $C_{K_{ses}}$ as D Rni $(C_{K_{ses}})$ (9)

Step2 Each SM_i will get $(K_{ses}||\mathrm{CHMeterID})$(10)

Step3 This K_{ses} will be used for secure data communication between SM_i and Gateway

4.7.3. Actual Data Communication

Step1$M =$ Readings | Commands at SM_i (11)

Step2 ComputeCi $= E_{K_{ses}}(M)$bySM_i(12)

Step3 Send Ci to CH

Step4 Data aggregation techniques will be applied on received C_i by CH as well as Gateway.

Step5 Aggregated C_i will be further send to computer systems at local management office over dedicated lines secured by IPSec or VPN tunnels.

4.8 Cluster-Head Rotation Phase

CH will be rotated as:

- After reaching to a specified amount of time T_{CH} (minutes)
- An $Error_{CH}$ causing to stop CH from working. In this case, a list ($\boldsymbol{CHErr\ i, Meter\ ID\ j, Remtime}$)will be formed containg CH Meter ID, its remaining time to provide services to cluster members

Following algorithm.2 performs CH rotation as:

Algorithm2. Cluster-Head Rotation

```
Start: Initialize counter=:0; Startup time=:00:00:00;  i=1;j=1;Errcounter=:0;Tsecs=:0; Remtime=:0
Input:  Read $T_{CH}$, k
Tsec=: ($T_{CH}$ * 60)
Read $_{\text{CH i, Meter ID j, Tsec}}$
Loop:  while (j <=k) do
Startup time=: Clock: Hour: Minutes: Seconds
Clock Tick++; Counter++
If ($CH_{\text{i, Meter ID j}}$ == Error && counter!= Tsecs) Then
Remtime=: Tsecs –counter
Add $CHErr_{\text{i, Meter ID j, Remtime}}$
Goto Loop
Else If (counter==Tsecs&& j<k) then
Initialize counter=:0; Startup time=:00:00:00
Goto Loop
ElseIf (Errcounter !=0 && j==k && counter==Tsecs) Then
Initialize j=1; k=: Errcounter; counter=:0
While (j<=k) do
Add $CH_{\text{i, Meter ID j, Tsec}}$= $CHErr_{\text{i, Meter ID j, Remtime}}$
End While
Goto Loop
Else
Goto Start
 End If; End If; End If
End While
Output: Return  $CH_{\text{i, Meter ID j, Tsec}}$
```

5Security Analyses

Our proposed scheme for AMI fulfills security requirements like as given below:

5.1 Device Authentication

Each device (Smart Meter and Gateway) identity will be checked at the Authentication systems at local management office as well as operation center before joining the communication network and getting the utility services. Illegal device won't be able access the communication network and utility services of the Smart Grid.

5.2 Confidentiality

Smart Meter data (readings & control commands) are kept private from inside and outside intruders by using ECC and AES encryption [14, 15] with secure session key exchange.

5.3 Data Integrity

To ensure integrity of Smart Meter data (readings & control commands), we usedSHA_{128} for computing message digest which will ensure that the data during transmission was not tampered [16].

5.4 Clusters-Head Rotation

CH rotation at regular intervals makes it difficult for an attacker to find out the main communication entity for various passive and active attacks.

6 Conclusions

AMI is an integral part of Smart Grid communication network and various communication topologies has been proposed with different security schemes from research community. In this paper, we proposed a new efficient communication architecture based on dynamic clustering for AMI in Smart Grid coupled with hybrid cryptosystem which ensures security features like confidentiality, integrity and privacy of metering data in AMI communication networks. The proposed solution incurs less computational and communication cost leading to better resources utilization.

REFERENCES

[1] Moslehi, K. and Kumar, R. “A reliability perspective of the smart grid”, IEEE Transactions on Smart Grid, 1(1), (2010), 57-64

[2] Li, F., Qiao, W., Sun, H., Wan, H., Wang, J., Xia, Y., and Zhang, P. “Smart transmission grid: Vision and framework”, IEEE Transactions on Smart Grid, 1(2), (2010), 168-177

[3] MSP430 for Utility Metering Applications, available at Texas Instruments, http://focus.ti.com/mcu/docs/mcuorphan.tsp?contentId=31498

[4] Yan, Y., Qian, Y., Sharif, H., and Tipper, D. “A survey on smart grid communication infrastructures: Motivations, requirements and challenges”, IEEE Communications Surveys & Tutorials, 15(1), (2013), 5-20.

[5] Yan, Y., Qian, Y., Sharif, H., and Tipper, D. “A survey on cyber security for smart grid communications”, IEEE Communications Surveys & Tutorials, 14(4), (2012), 998-1010.

[6] Deng, P., and Yang, L. “A secure and privacy-preserving communication scheme for Advanced Metering Infrastructure”, In Innovative Smart Grid Technologies (ISGT), (2012), 1-5

[7] Yan, Y., Qian, Y., and Sharif, H. “A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid”, In Wireless Communications and Networking Conference (WCNC), (2011), 909-914

[8] Kamto, J., Qian, L., Fuller, J., and Attia, J. “Light-weight key distribution and management for advanced metering infrastructure”, In GLOBECOM Workshops (GC Wkshps), (2011), 1216-1220

[9] Lu, R., Liang, X., Li, X., Lin, X., and Shen, X. Eppa “An efficient and privacy-preserving aggregation scheme for secure smart grid communications”, IEEE Transactions onParallel and Distributed Systems, 23(9), (2012), 1621-1631

[10] Nicanfar, H., Jokar, P., Beznosov, K., and Leung, V. C. “Efficient authentication and key management mechanisms for smart grid communications”, In IEEE System Journal, (2013) 1-12

[11] Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R., and Shen, X. “A lightweight message authentication scheme for smart grid communications”, IEEE Transactions on Smart Grid, 2(4), (2011), 675-685

[12] Yan, Y., Hu, R. Q., Das, S. K., Sharif, H., and Qian, Y. “An efficient security protocol for advanced metering infrastructure in smart grid”, IEEE Network, 27(4), 2013

[13] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. P. “Smart grid technologies: communication technologies and standards”, IEEE transactions on Industrial informatics, 7(4), (2011), 529-539

[14] Amin, N., Asad, M., Nizamuddin, & Chaudhry, S. A. “An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem”, 9th IEEE International Conference Networking, Sensing and Control (ICNSC),(2012), 118-121

[15] Iqbal, J., Nizamuddin, Amin, N., and Umar, A. I. “Authenticated Key Agreement And Cluster Head Selection For Wireless Body Area Networks” In 2nd National Conference onInformation Assurance (NCIA), (2013), 113-117

[16] Ch, S. A., Nizamuddin, and Sher, M. “Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem”, In Information Systems, Technology and Management (2012), 135-142

[17] Zakarya, M. “SMART GRIDS: A prologue & unscrew challenges that needs to be addressed, A Short Survey on how to make Grids Smarter”, VAWKUM Transaction on Computer Sciences, 1(1), 2013